January 26, 2000

Boxes ...

Background

I try to write a course diary recording what happened during each class meeting. Part of the diary entry for our second class meeting follows:

> I then displayed a different kind of encryption scheme, by writing a rectangular 3 by 5 array on the board, and writing horizontally the message `the giraffe hops`, padding it appropriately on the end with an `x` and reading off vertically the message `trhhaoefpgfsiex` (see the illustration below).
>
> ```
> thegi
> raffe
> hopsx
> ```
>
> I described how Bob would decipher, insisting that his instructions be as unambiguous as possible and as similar to Alice's as possible. So the key in this case was the pair of numbers (3 & 5) which Alice used and which Bob reversed.
>
> This is one example of a transposition method, where letters were permuted or interchanged.

Reality (?)

Alice might send the messages below to Bob using this system. What are the plaintexts corresponding to each of the ciphertexts? I have tried to make this exercise a bit realistic by allowing Alice to commit some simple mistakes. In each case the message has been split into groups of 5 letters, which is conventional in this field. Briefly explain any problems you find and describe how you solved them. Please hand in your work Monday. People may work together and hand in joint solutions. Of course you should indicate the members of your group.

Message A The key is 4 & 6. The message is

`twash fncea dosli inltd osix`

Message B The key is 3 & 9. The message is

`tsnhf iergr ohizt veenr tio`

Message C The key is 4 & 10. The message is

`wtump wdlar hhnet owbrx eecsh riemx nsoue llwex`

Message D The key is [illegible] & 1[illegible]. The message is

`tehhy hheef eowwi wwoie olonr liddc vnsie egasx sinvx andex rttrx`

Message E The key is 6 & 4. The message is

`segwu uhlsi cnoin cnoin shxvn omfx`

Hints are available electronically. Hints are available electronically. Hints are available electronically. Hints are available electronically. Hints are available electronically. Hints are available electronically.